# STEGANOGRAFI PADA CITRA DIGITAL DENGAN METODE CATMAP DAN OUTGUESS

**Bahtera Alam Wijaksono**
Program Studi Teknik Informatika, Univrsitas Indraprasta PGRI
Email: bahtera.alam.w@gmail.com

**Abstrak**

Menyisipkan pesan dalam sebuah gambar atau lebih sering dikenal dengan istilah *steganografi* dimana pengembangan dari metode *kriptografi* yang sudah dikenal sebelumnya. Metode dengan s*teganografi* dapat dikatakan lebih baik dibandingkan dengan sebelumnya *kriptografi*. Pada penggunan metode *steganografi* tidak sebatas dengan hanya pada satu metode. Pada beberapa metode digunakan dalam untuk mendapatkan gambar stego atau stego image yang lebih aman, tidak jauh berbeda dengan aslinya hingga tidak mudah untuk di pecahkan atau dicurigai oleh orang lain yang tidak memiliki hak akses terhadap file tersebut. Beberapa metode yang telah ada, tentunya masing-masing metode memiliki kelebihan dan kekurangan. Metode yang dibandingkan antara lain metode *Least Significant Bit* (LSB) dan *End Of File* (EOF). Kedua metode ini merupakan metode yang sering digunakan untuk pengembangan. LSB adalah metode lama yang terus menjadi dasar untuk menciptakan metode-metode baru lainnya, seperti halnya EOF yang merupakan pengembangan dari metode LSB. Melalui penelitian ini penulis menganalisis metode mana yang lebih efektif dan efisien untuk menyembunyikansebuah pesan singkat dalam bentuk format text. Selain itu, dari hasil penelitan penulis ingin mengembangkan aplikasi *steganografi*. Melihat dan mempelajari kedua metode tersebut diharapkan pengembangan yang dilakukan akan lebih baik dan dapat menutupi kekurangan sebelumnya.
**Kata Kunci:** *Steganografi, Kriptografi*, LSB, EOF, Arnold Cat Map, Outguess

***Abstract***

*Steganography more commonly known as hiding some message in a picture, on this methods that have previously known as cryptographic. Development methods steganography more better then cryptographic, where method steganographic not limited to only one method. On case using file images or call stego images more secure and suspected by others who do not have assess right to the files. Method be compare of Least Significant Bit (LSB) and the End Of File (EOF)of course, each method has advantages and disadvantages Through this researchanalyze which method is more effective and efficient to hide a short message in the form of text format. In addition, the results of the literature study authors wanted to develop the application of steganography. See and learn both methods is expected that development will do better and be able to cover the shortfall the previous.*
***Keyword:*** *Steganografi, Kriptografi, LSB, EOF, Arnold Cat Map, Outguess*

## Pendahuluan

Citra merupakan bentuk penyajian suatu data dalam bentuk visual. Peranan citra dalam industri multimedia saat ini sangat memegang peranan penting. Seperti yang kita ketahui *file* berbentuk video sebenarnya tersusun atas rangkaian dari beberapa frame citra yang ditampilkan dalam tempo yang cepat.

Sampai saat ini citra tidak hanya disimpan dalam media penyimpanan seperti *Harddisk*, akan tetapi citra juga beredar dalam suatu jaringan internet. Penyimpanan ataupun peredaran citra dalam suatu jaringan internet ini rawan atas pengaksesan atau penyadapan oleh pihak-pihak yang tidak memiliki otoritas yang legal. Oleh karena itu, untuk menghindari hal tersebut dan juga untuk mengamankan suatu citra dikenal suatu proses enkripsi dari citra yang dinamakan kriptografi.

Kriptografi adalah suatu ilmu dan seni yang digunakan untuk menjaga kerahasiaan suatu berita ataupun data. Akan tetapi, kebanyakan algoritma yang digunakan dalam kriptografi ini ditujukan hanya untuk mengenkripsi suatu data. Seperti contohnya algortima DES, AES, blowfish, RC4, RSA dan lain-lain. Dalam perkembangannya suatu citra sekarang memiliki volume yang kecil. Algoritma pengenkripsian di atas memerlukan waktu komputasi yang cukup lama untuk melakukan enkripsi terhadap data yang memiliki volume yang cukup besar. Untuk kebutuhan aplikasi yang real time seperti *teleconference*, *live video streaming*, dan lain-lain yang biasanya memiliki volume data yang besar, jelas terlihat jika algoritma pengenkripsian yang konvensional kurang cocok untuk digunakan Struss (2009).

Karena alasan-alasan spesifik di atas, maka perlu dikembangkan algoritma yang khusus untuk citra digital. Penelitian tentang enkripsi citra dilakukan dengan intensif. Para peneliti telah banyak mengembangkan algoritma enkripsi citra digital. Menurut Younes (2008), kebanyakan algoritma-algoritma enkripsi citra dapat dikelompokkan menjadi dua kelompok. Kelompok pertama adalah algoritma enkripsi selektif non-chaos, sedangkan kelompok kedua adalah algoritma enkripsi selektif atau non-selektif yang berbasis chaos.

Yang dimaksud dengan algoritma selektif adalah algoritma yang mengenkripsi hanya sebagian elemen di dalam citra namun efeknya citra terenkripsi secara keseluruhan. Tujuan algoritma enkripsi selektif adalah mengurangi volume komputasi, yang konsekuensinya adalah menghemat waktu proses enkripsi. Enkripsi selektif cocok untuk aplikasi yang membutuhkan persyaratan real-time. Kriptografi berbasis chaos menjadi topik penelitian yang atraktif saat ini. Chaos digunakan di dalam kriptografi karena tiga alasan: (1) sifat chaos yang sensitif terhadap kondisi awal sistem, (2) chaos berkelakuan acak, dan (3) nilai-nilai chaos tidak memiliki periode. Review beberapa algoritma enkripsi citra dengan menggunakan skema chaos dapat dibaca di dalam Sharma (2010).

Kehadiran beberapa jejaring sosial yang sedang marak saat ini, seperti facebook, twitter, myspace, dll membuat proses pengenkripsian ini sangat dibutuhkan dan berguna. Setiap orang dapat menyimpan suatu pesan yang bagi sebagian orang pesan itu hanya sekedar bentuk file (gambar, musik, video, dll), akan tetapi di lain pihak orang lain dapat mengambil pesan rahasia yang disisipkan ke dalam file tersebut.

Steganografi dapat diterapkan dalam beberapa bentuk data digital, misalnya teks, citra (gambar), suara, dan bahkan video. Akan tetapi sampai saat ini yang umum digunakan untuk pengembangan aplikasi steganografi adalah gambar dan suara. Oleh karena itu, dalam penelitian ini akan dibahas suatu teknik steganografi menggunakan salah satu dari algoritma Chaos (CatMap) dan juga dengan menggunakan algoritma OutGuess.

Tujuan dari penelitian ini adalah untuk mengetahui perbandngan kinerja antara metode steganografi menggunakan algoritma CatMap dan juga dengan yang menggunakan algoritma OutGuess.

## Tinjauan Pustaka

### CAT MAP

*Arnold Cat Map* (*ACM*) merupakan fungsi *chaos* dwimatra dan bersifat *reversible*. Fungsi *chaos* ini ditemukan oleh Vladimir Arnold pada tahun 1960, dan kata "*cat*" muncul karena dia menggunakan citra seekor kucing dalam eksperimennya. *ACM* mentransformasikan koordinat $(x, y)$ di dalam citra yang berukuran $N \times N$ke koordinat baru $(x', y')$. Persamaan iterasinya adalah:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod(N)$$

dalam hal ini $(x_i, y_i)$ adalah posisi *pixel* di dalam citra, $(x_{i+1}, y_{i+1})$ posisi *pixel* yang baru setelah iterasi ke-$i$; $b$dan $c$adalah *integer* positif sembarang. Determinan matriks

$$\begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}$$

harus sama dengan 1 agar hasil transformasinya bersifat *area-preserving*, yaitu tetap berada di dalam area citra yang sama. *ACM* termasuk pemetaan yang bersifat satu-kesatu karena setiap posisi *pixel* selalu ditransformasikan ke posisi lain secara unik. *ACM* diiterasikan sebanyak $m$kali dan setiap iterasi menghasilkan citra yang acak. Nilai $b$, $c$, dan jumlah iterasi $m$dapat dianggap sebagai kunci rahasia.

Proses yang terjadi di dalam setiap *iterasi ACM* adalah pergeseran (*shear*) dalam arah $y$, kemudian dalam arah $x$, dan semua hasilnya (yang mungkin berada di luar area gambar) dimodulokan dengan $N$agar tetap berada di dalam area gambar (*area preserving*) Setelah *ACM* diiterasi sebanyak $m$kali, maka terdapat $T$sedemikian sehingga $(x_T, y_T) = (x, y)$, yang dalam hal ini nilai $T$bergantung pada $b$, $c$, dan ukuran $N$ We-bin (2009).

Ini berarti sesudah *ACM* diiterasi sebanyak $T$kali, maka hasil iterasinya kembali ke citra semula, sehingga dikatakan *ACM* besifat *reversible* dan periodenya adalah $T$. Menurut Struss. (2009), penelitian Freeman J. Dyson dan Harold Falk menemukan bahwa $T < 3N$. Gambar 1 memperlihatkan iterasi *ACM* terhadap citra 'burung'. Pada iterasi ketiga hasilnya sudah terlihat seperti citra acak, semakin banyak iterasinya citra hasil semakin acak (dalam hal ini *ACM* telah berada dalam fase *chaos*). Jika proses iterasi diteruskan maka hasilnya kembali menuju citra semula. Pada contoh ini citra 'burung' kembali ke bentuk semula pada iterasi ke- $192$ sehingga dikatakan periodenya adalah $T = 192$. Gambar 1. Iterasi ACM pada citra 'burung' dengan periode $T = 192$.

Seperti umumnya fungsi *chaos* yang bersifat deterministik, citra yang sudah teracak oleh *ACM* dapat direkonstruksi menjadi citra semula dengan menggunakan kunci yang sama ($b$, $c$, dan $m$). Persamaan iterasinya adalah

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}^{-1} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod(N)$$

Setelah iterasi terakhir citra hasil sama seperti citra semula. Proses dekripsipun selesai.

**OutGuess**

Algoritma steganografi OutGuess diusulkan oleh Neils Provos untuk melawan serangan chi-square. Dalam tahap awal algoritma ini mirip dengan J-Steg, Outguess adalah perangkat steganografi universal yang memungkinkan penyisipan informasi rahasia ke dalam sumber data apapun (tidak harus gambar) yang memiliki bit redundan. Program ini memerlukan handler yang spesifik terhadap data yang akan mengekstrak bit-bit redundan dan menuliskannya kembali setelah diadakan modifikasiXiang, dkk. (2007).

Steganografi menyembunyikan adanya komunikasi. Sistem steganografi klasik bergantung pada menjaga kerahasiaan sistem enkoding, sedangkan steganografi modern hanya dapat dideteksi jika informasi rahasia berupa kunci rahasia tertangkap. Karena sifat sistemnya yang menyusup ke dalam, steganografi meninggalkan jejak dalam karakteristik dari medium penyimpanannya. Jejak tersebut dalam file JPEG adalah distribusi bit dalam daerah Terdeteksinya jejak tersebut memberikan peluang bagi pihak ketiga untuk menemukan file mana yang sudah diubah, menandakan bahwa ada komunikasi rahasia yang sedang berlangsung. Walaupun isinya tetap rahasia, tapi sifat tersembunyi tersebut jadi diketahui.

Pada gambar berformat JPEG, Outguess menjaga statistik berdasarkan hitungan frekuensi. Oleh karena itu tes statistik tidak akan bisa menentukan ada atau tidaknya penyembunyian data. Sebelum memasukkan data ke gambar, Outguess dapat mengukur berapa besar pesan yang dapat ia sembunyikan selagi mempertahankan statistikZhang, dkk. (2006).

OutGuess menggunakan objek iterator umum untuk memilh bit mana yang harus dimodifikasi. Sebuah seed bisa dimanfaatkan untuk mengatur perilaku iterator. Perubahan disimpan di dalam data bersama dengan sisa dari pesan tersebut. Dengan mengubah seednya, OutGuess mencoba mencari sebuah urutan bit yang memiliki banyak perubahan minimal.

## Metodologi Penelitian

Langkah-langkah yang dilakukan dalam penelitian adalah sebagai berikut:

1. Gambar
   Pada pengujian file gambar dengan satu object gambar yang sama akan tetapi dibuat seperti mempunyai ukuran dan dimensi yang cukup beda-beda, lebih jelasnya dapat dilihat pada tabel berikut ini:

**Tabel 1. Pengujian File Gambar**

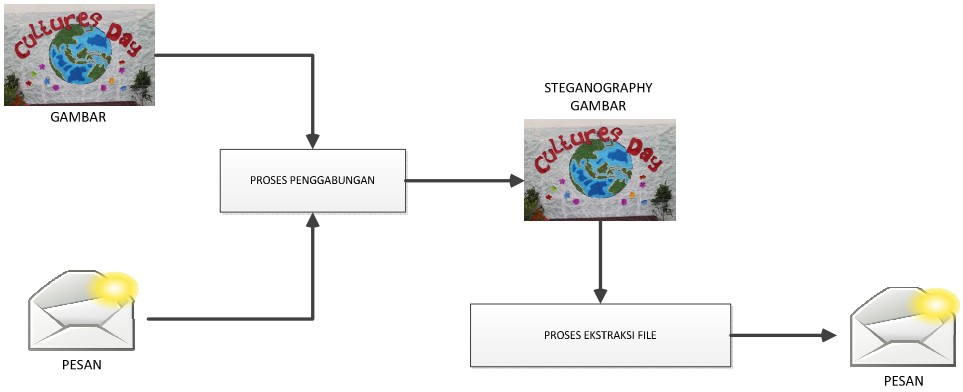
| NO | Image File | | |
|---|---|---|---|
| | Nama File | Dimensi | Size |
| 1 | Gambar1.jpg | 640 X 427 | 85.1 KB |
| 2 | Gambar2.jpg | 800 X 534 | 128 KB |
| 3 | Gambar3.jpg | 800 X 534 | 128 KB |
| 4 | Gambar4.jpg | 1600 X 1067 | 391 KB |
| 5 | Gambar5.jpg | 1600 X 1067 | 391 KB |
| 6 | Gambar6.jpg | 1600 X 1067 | 391 KB |

2. Text File
   Pada penggujian file text menggunakan file 6 (enam) dengan format (TEXT) dimana file text yang akan disisipkan diberikan sebuah informasi yang dijadikan sebagai alat pengujian yang akan digunakan dalam pengujian, lebih jelasnya dapat dilihat pada table berikut ini:

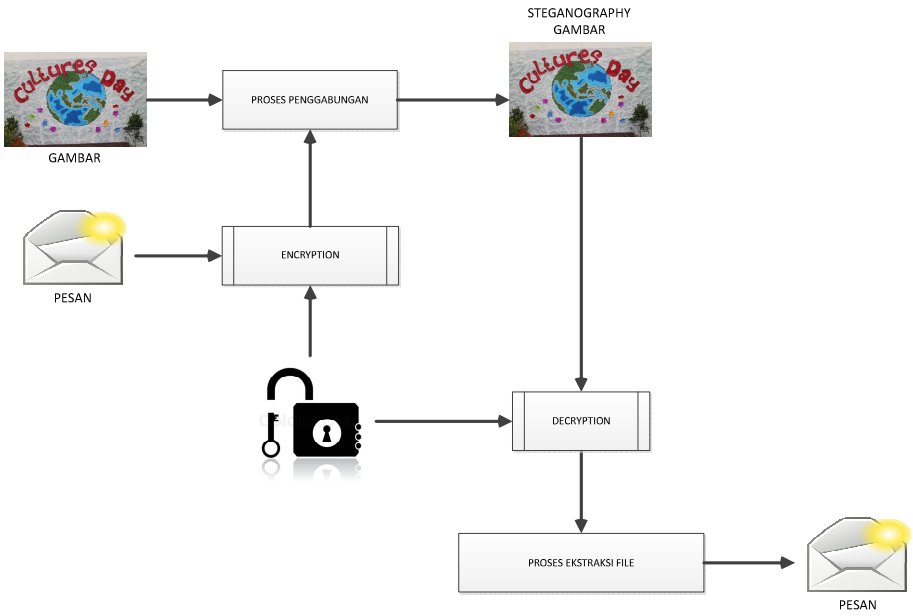
**Tabel 2. Pengujian File Text**

| NO | Text File | |
|---|---|---|
| | Nama File | Size |
| 1 | Text1.txt | 1.5 KB |
| 2 | Text2.txt | 1.5 KB |
| 3 | Text3.txt | 10.8 KB |
| 4 | Text4.txt | 1.5 KB |
| 5 | Text5.txt | 5.3 KB |
| 6 | Text6.txt | 10.8 KB |

3. Pengujian *diagram cat maps design* dan *diagram outguess design*
   Setelah langkah satu dan dua sudah disiapkan barulahdapat melakukan tahapan untuk melakukan pengujian pada file tersebut dengan menggunakan *catmaps* dan *outguess.*
   Berikut tahapan pengujian *diagram cat maps design* dan *diagram outguess design* yang dilakukan, dimana tiap file gambar dan text mendapatkan perlakukan yang sama, dimana hasil dari pengujian tersebut menghasilkan sebuah file images, dikarenakan pada tahapan ini melakukan pengujian terhadap 6 (enam) file gambar dan text maka terdapat hasil 6 keluaran berupa images atau bisa disebut *steganography images*.




**Gambar 1. Pengujian Cat Maps Design**




**Gambar 2. Pengujian OutGuess Design**

## Hasil dan Pembahasan

Pada penelitian ini, digunakan dalam pengujian tiap file gambar dan file dikompare dengan menggunakan catmap dan outguess secara bersamaan pada hasil dari melakukan kompre tersebut mendapatkan hasil yang cukup signifikan.

Pada hasil yang diperoleh dari pengujian dengan 6 file terdapat perubahan ukuran pada images file yang di ujicobakan dapat dilihat pada Tabel 3 dengan menggunakan catmap dan hasil dengan menggunakan outguess padaTabel 4.

p-ISSN: 2527 – 9661
e-ISSN: 2549 – 2837

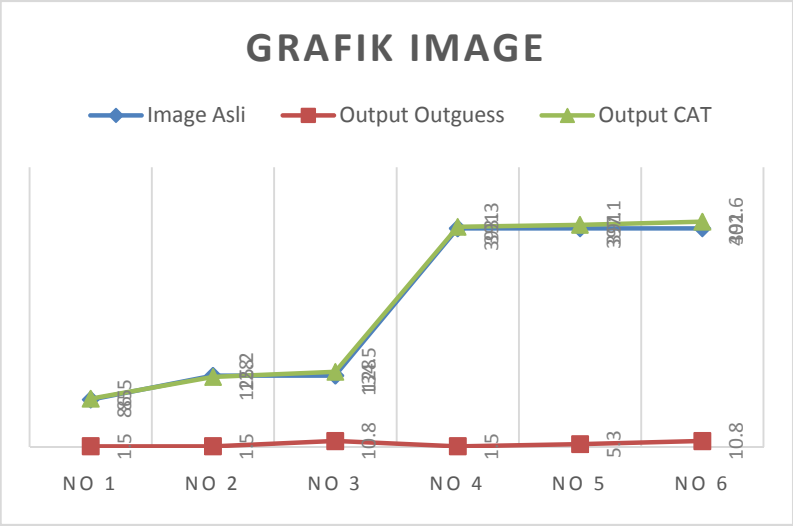
**Tabel 3. Hasil diperoleh dengan Catmap**

| KETERANGAN | CAT Map | | | | | |
|---|---|---|---|---|---|---|
| | File 1 | File 2 | File 3 | File 4 | File 5 | File 6 |
| Name File | Gambar1 | Gambar2 | Gambar3 | Gambar4 | Gambar5 | Gambar6 |
| Extension | JPG | JPG | JPG | JPG | JPG | JPG |
| Dimension | 640 X 427 | 800 X 534 | 800 X 534 | 1600 X 1067 | 1600 X 1067 | 1600 X 1067 |
| Resolution | 96 dpi | 96 dpi | 96 dpi | 96 dpi | 96 dpi | 96 dpi |
| Bit Depth | 24 | 24 | 24 | 24 | 24 | 24 |
| Resolution Unit | 0 | 0 | 0 | 0 | 0 | 0 |
| Size | 86,5 Kb | 125.2 Kb | 134.5 Kb | 393.3 Kb | 397.1 Kb | 402.6 Kb |

**Tabel 4. Hasil diperoleh Out Guess**

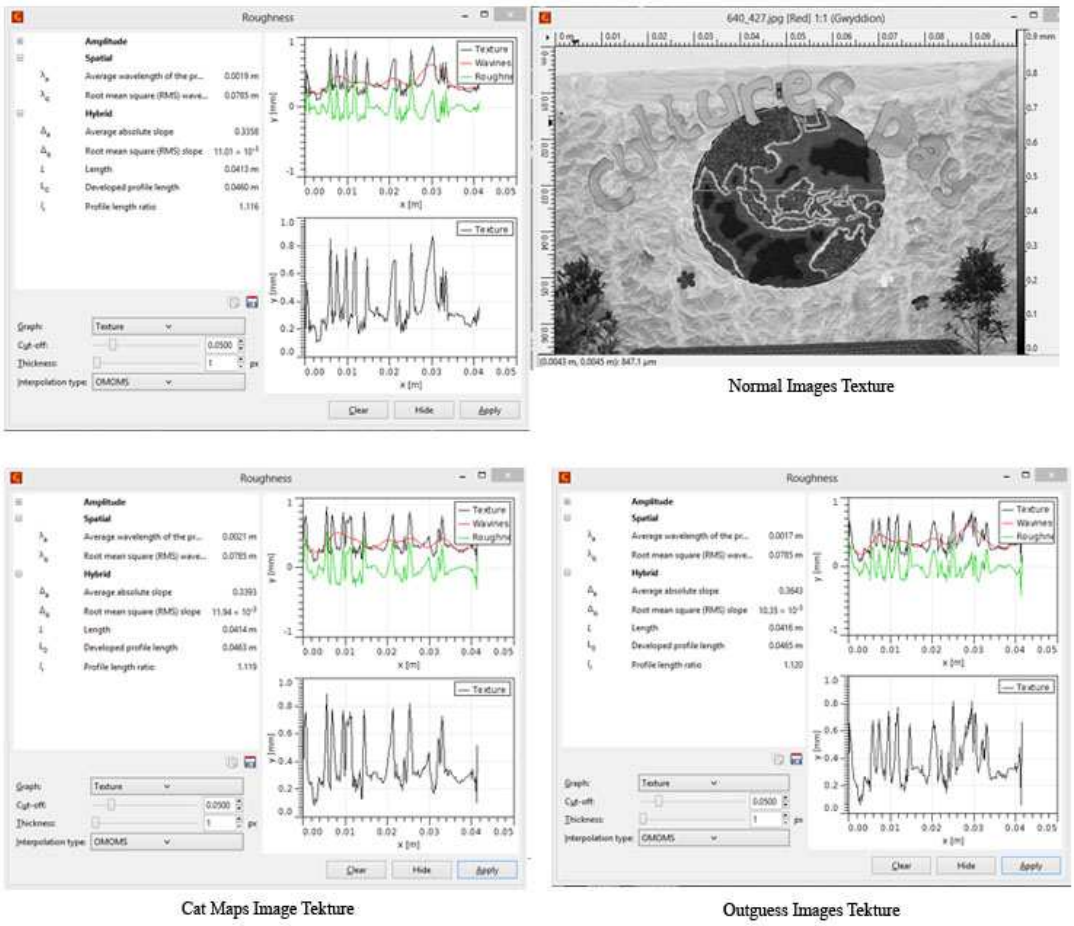
| KETERANGAN | OutGuess | | | | | |
|---|---|---|---|---|---|---|
| | File 1 | File 2 | File 3 | File 4 | File 5 | File 6 |
| Name File | Gambar1 | Gambar2 | Gambar3 | Gambar4 | Gambar5 | Gambar6 |
| Extension | JPG | JPG | JPG | JPG | JPG | JPG |
| Dimension | 640 X 427 | 800 X 534 | 800 X 534 | 1600 X 1067 | 1600 X 1067 | 1600 X 1067 |
| Resolution | 96 dpi | 96 dpi | 96 dpi | 96 dpi | 96 dpi | 96 dpi |
| Bit Depth | 24 | 24 | 24 | 24 | 24 | 24 |
| Resolution Unit | 0 | 0 | 0 | 0 | 0 | 0 |
| Size | 58,1 Kb | 85,5 Kb | 85,5 Kb | 280 Kb | 280 Kb | 281 Kb |

Dari beberapa hasil penggujian yang menggunakan outguess menghasilkan file yang relative lebih kecil dibandingkan dengan ukuran images yang sebenarnya dan hasil kualitas gambar yang dihasilkan relative kurang, sedangkan dengan mengunakan catmaps tidak terdapat perubahan pada hasil kualitas images akan tetapi file images tersebut menjadi lebih besar dari images aslinya dapat dilihat pada Gambar 3.




**Gambar 3. Grafik Perbandingan Data Asli dengan Data Hasil Pengujian**

Hasil dari pengujian tersebut yang sebelumnya menghasilkan masing-masing 6 file dari catmaps dan outguees, dari hasil pengujian tersebut diambil 1 sampel file dimana sampel tersebut akan dijadikan bahan analisa. Sampe file tersebut akan akan dibedakan dengan file aslinya, untuk proses analisa file tersebut menggunakan alat bantu tools analisa gambar. Pada hasil akhir dari analisa menggunakan tools tersebut menghasilkan suatu data yang cukup berbeda dengan file asli sedangkan dengan dengan catmaps terdapat perubahan pada akhir grafik sedangkan dengan outguess tiap-tiap grafik yang dihasilkan sangat berbeda dengan yang asli. berikut hasil dengan menggunakan tools analisa gambar dapat dilihat pada Gambar 4.




**Gambar 4. Hasil Analisa Images dengan Roughness**

## Simpulan dan Saran

Hasil percobaan dengan menggunakan catmap dan outguess terdapat beberapa kelebihandan kekurangan dimana kelebihan dengan menggunakan catmap gambar yang dihasilkansesuai dengan asli dan tidak ada perubahan akan tetapi untuk size dan tekture gambar dihasilkan terdapat perubahan. Sedangkan dengan menggunakan outguess dimana size yang dihasilkan lebih kecil, sedangkan secara kualitas gambar yang dihasilkan juga ikut menurun dan pada grafik tekture yang dihasilkan juga mengalami perubahan.

## Daftar Pustaka

Sharma. (2010). Image Encryption Technique Using Chaotic Schemes: A Review, International Journal of Engineering. *Science and Technology,* Vol 2 (6) 2010.

Wei-bin. (2009). *Image Encryption Algorithm Based on Henon Chaotic System.* Proceeding of International Conference on Image Analysis and Signal Processing (IASP 2009).

Struss. (2009). *A Chaotic Image Encryption*, Mathematics Senior Seminar, University of Minnesota.

Zhang, dkk. (2006). Chaotic Scrambling Algorithm Based on S-DES. *Journal of Physics: Conference Series* 48, 349-353.

Xiang, dkk. (2007). Selective Image Encryption Using a spatiotemporal Chaotic System, *Chaos* Volume 17.